

CUSTOMER NO.: 24498
Serial No.: 10/602,754
Final Office Action dated: 10/10/07
Date of Response: 10/07/07

PATENT
PU030107

RECEIVED
CENTRAL FAX CENTER

DEC 07 2007

REMARKS/ARGUMENTS

This application has been reviewed in light of the Final Office Action dated October 10, 2007.

Claims 1-19 are pending in the application. The claims presented herewith are unamended. The Examiner's reconsideration of the rejection in view of the following remarks is respectfully requested.

By the Office Action, claims 1-8, 10 and 12-19 stand rejected under 35 U.S.C. §102(b) as being anticipated by McMullan, Jr., et al. (U.S. Patent No. 5,654,746) (hereinafter 'McMullan').

Prior to addressing the outstanding rejections, the Applicants will briefly summarize aspects of the present principles to better assist the Examiner in appreciating the differences between claimed features and the prior art. In accordance with an aspect of the present principles a service provider may remotely access and modify stored information on a user-access device across a distributed network (see, e.g., Specification, p. 5, lines 17-21). In one implementation of the present principles, the service provider may designate portions of the stored information to be inaccessible by the user (see, e.g., Specification, p. 3, line 28 to p. 4, line 2). This feature ensures that users are prevented from accessing information that may potentially compromise the service provider's internal security standards (see, e.g., Specification, p. 3, line 28 to p. 4, line 2). Additionally, the information that is designated inaccessible to a user may be accessed by the service provider (Specification, p. 5, lines 1-3; p. 5, lines 32-35; 108, Fig. 2). Such access may be necessary to adequately provide services to a user. For example, a service provider may be required to access a configuration file to establish a communication link between a user-device and a network (see, e.g., Specification, p. 3, lines 26-30).

Claims 1 and 10 include at least some of the features described above. Claim 1 includes, inter alia: “[a] security system for use in a distributed network, comprising: . . . control mechanism disposed at a location of the service provider which accesses and modifies stored information on each access device of the end users to designate service provider-accessible portions of the information to prevent access thereof by the end users.” Similarly, claim 10 includes, inter alia: “[a] method for maintaining system security for a network service provider,

CUSTOMER NO.: 24498
Serial No.: 10/602,754
Final Office Action dated: 10/10/07
Date of Response: 10/07/07

PATENT
PU030107

comprising the steps of: . . . remotely accessing and modifying the end user network devices to designate service provider-accessible information stored on the access devices; and preventing the end user from accessing the designated service provider-accessible information on the end user's access device."

Thus, the portions of stored information recited in claims 1 and 10 include two attributes: a) the portions of the stored information are remotely designated by the service provider to prevent access thereof by end-users; and b) the designated portions of information are accessible by the service provider.

McMullan does not disclose that any portions of information stored on a user device have both of these attributes. McMullan describes a game delivery system in which games are downloaded from a service provider to a home game adapter (see McMullan, Fig. 1; column 7, lines 9-12). A user may download games upon purchasing time for temporary play (McMullan, column 10, line 58 to column 11, line 12). To manage user access to the downloaded games, the service provider accesses a pay to Pay-to-Play (PTP) table located in the home game adapter (McMullan, column 11, lines 45-62). Upon expiration of the user-purchased time, the system of McMullan institutes a "reset" operation in the home game adapter to halt game play, wherein all registries are cleared, requiring a user to initiate a new download if she so wishes play the game again (e.g., McMullan, column 7, lines 55-61; column 17, lines 2-4; column 12, lines 23-27). In addition, as pointed out by the Examiner, the service provider may also access a user device to set a new adapter address, to set an adapter timeout setting routine, and to perform other transactions (see, e.g., McMullan, column 17, lines 38-56).

However, portions of the information stored on a user-device described in McMullan are not both: a) remotely designated by the service provider to prevent access thereof by end-users; and b) also accessible by the service provider. The PTP table and stored information related to adapter address, a timeout setting routine, etc. are not remotely designated by the service provider to be inaccessible to end-users. Moreover, while a service provider may prevent a user from accessing a downloaded game by performing a reset operation, McMullan does not disclose that the downloaded game data program is accessible by the service provider after the reset. As stated above, every time a reset operation is made, all registries are cleared and the user is required to

CUSTOMER NO.: 24498
Serial No.: 10/602,754
Final Office Action dated: 10/10/07
Date of Response: 10/07/07

PATENT
PU030107

initiate a new download. Thus, McMullan fails to anticipate claims 1 and 10 at least because McMullan does not disclose that portions of stored information are both remotely designated by the service provider to prevent access thereof by end-users; and also accessible by the service provider.

Furthermore, modifying McMullan to include portions of stored information with both of the above-described attributes is not obvious. Firstly, as the Examiner has admitted, configuration information in a user-device cannot be read by the user. Accordingly, there is no reason to remotely designate portions of such information to be inaccessible by a user. Secondly, modifying the McMullan system to permit service provider access to a designated game is also not obvious, as there is also no reason for a service provider described in McMullan to access a game downloaded to a user device after the purchased time of use expires.

Therefore claims 1 and 10 are believed to be patentable over McMullan for at least the reasons stated above. Moreover, claims 2-8 and 12-19 are believed to be patentable due at least to their dependencies from claims 1 and 10.

Claims 9 and 11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over McMullan. Independent claims 1 and 10 are believed to be patentable over McMullan for at least the reasons stated above. Accordingly, claims 9 and 11 are believed to be patentable due at least to their dependencies from claims 1 and 10, respectively.

CUSTOMER NO.: 24498
Serial No.: 10/602,754
Final Office Action dated: 10/10/07
Date of Response: 10/07/07

PATENT
PU030107

RECEIVED
CENTRAL FAX CENTER

DEC 07 2007

CONCLUSION

In view of the foregoing, the applicants respectfully request that the rejections of the claims set forth in the Office Action of October 10, 2007 be withdrawn, that pending claims 1-19 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicants' representatives Deposit Account No. 07-0832.

Respectfully submitted,

LARRY CECIL BROWN ET AL.

By:


Jeffrey D. Hale, Attorney
Registration No. 40,012
(609) 734-6444

JDH:pdf

Thomson Licensing LLC
2 Independence Way, Suite #200
P. O. Box 5312
Princeton, NJ 08543-5312

December 7, 2007